

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0661845 A3

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.03.2000 Bulletin 2000/09

(51) IntCl. 7: **H04L 9/32, H04L 9/30**

(43) Date of publication A2:
05.07.1995 Bulletin 1995/27

(21) Application number: 94309658.6

(22) Date of filing: 21.12.1994

(84) Designated Contracting States:
DE FR GB

• Naor, Simeon
Tel-Aviv, 69122 (US)

(30) Priority: 29.12.1993 US 175024

(74) Representative: Moss, Robert Douglas
IBM United Kingdom Limited
Intellectual Property Department
Hursley Park
Winchester Hampshire SO212JN (GB)

(71) Applicant: International Business Machines Corporation
Armonk, N.Y. 10504 (US)

(72) Inventors:
• Dwork, Cynthia
Palo Alto, California 94301 (US)

(54) **System and method for message authentication in an non-malleable public-key cryptosystem**

(57) A method is provided for authentication of encrypted messages (M). An non-malleable public-key encryption technique is employed, so that an eavesdropper (B) cannot employ an encrypted message (M), previously overheard, to generate a message which, when sent to a recipient (R), which would pass as a message originating from a valid sender (S). In a preferred embodiment, a protocol is provided in which, in response to a message authentication request (req) from a sender, a recipient (R) sends the sender (S) a string (st), encrypted according to the sender's non-malleable public key (Es). The sender (S) decrypts the string using its private key, and sends the recipient (R) a message (Auth(M, ST)) which is a function (Auth) of the string (St) and the message (M) to be authenticated. Because of the non-malleability of the public keys, an eavesdropper cannot impersonate the sender (S) or the recipient (R) and produce a disinformation message which would nevertheless contain the correct authorization string.

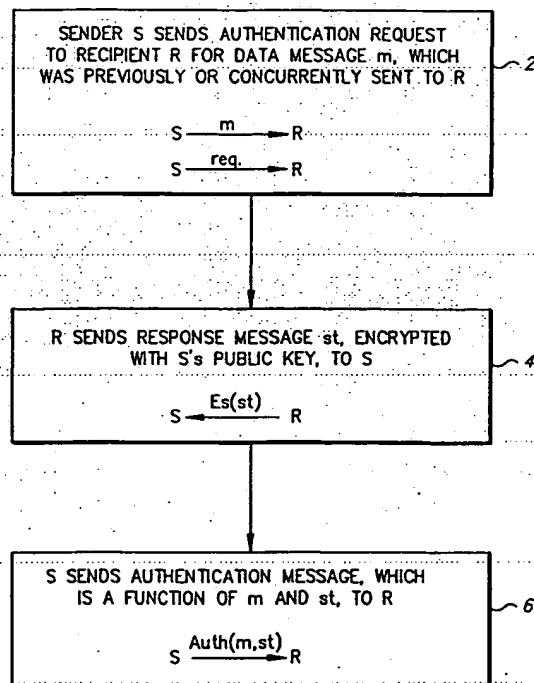


FIG. 2

EP 0 661 845 A3

Best Available Copy



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 30 9658

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 522 473 A (MITSUBISHI ELECTRIC CORP) 13 January 1993 (1993-01-13) * abstract * * column 1, line 50 - column 2, line 20 * * column 4, line 52 - column 7, line 2 * * claim 1 * * figures 2,4 *	1,2,4,5	H04L9/32 H04L9/30
A	SIMMONS G J: "A PROTOCOL TO PROVIDE VERIFIABLE PROOF OF IDENTITY AND UNFORGEABLE TRANSACTION RECEIPTS" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,US,IEEE INC. NEW YORK, vol. 7, no. 4, page 435-447 XP000007982 ISSN: 0733-8716 * abstract * * page 436, right-hand column, line 6 - line 20 * * page 437, right-hand column, line 3 - line 33 * * page 439, right-hand column, line 22 - page 442, right-hand column, line 47 *	1-6	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 10 January 2000	Examiner Gautier, L
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03 02 (P04C01)

Best Available Copy

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 94 30 9658

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

10-01-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0522473 A	13-01-1993	JP 2671649 B	29-10-1997
		JP 5012321 A	22-01-1993
		DE 69224238 D	05-03-1998
		DE 69224238 T	20-05-1998
		US 5245657 A	14-09-1993

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Best Available Copy